**ABSTRACT**

A message authentication system for generating a message authentication code (MAC) uses a single iteration of a keyed compression function when a message fits within an input block of the compression function, thereby improving efficiency. For messages that are larger than a block, the MAC system uses nested hash functions. The MAC system and method can use portions of the message as inputs to the nested hash functions. For example, the message authentication system can split the message into a first portion and a second portion. A hash function is performed using the first portion of the message as an input to achieve an intermediate result, and a keyed hash function is performed using a second portion of the message and the intermediate result as inputs. Thus, less of the message needs to be processed by the inner hash function, thereby improving efficiency, especially for smaller messages.